# 7. Best Practice

## 7.1 Introduction

The purpose of this chapter is to list a number of useful hints and guidelines for both Flexterminal developers and developers of cash register systems interfacing Flexterminals.

Although this chapter is an integrated part of the “Technical Reference Guide – Open Terminal Requirement Specification”, it may be seen as a separate description or summary of items worth paying special attention.

## 7.2 Documentation

For both stand–alone terminals and implementations where the terminal is connected to a cash register system, a user manual shall be provided by the terminal supplier.

This manual shall contain sufficient information making the staff able to operate system concerning card payments and settlements.

The manual shall also contain relevant technical information, including guidelines for PSAM replacement.

## 7.3 Terminal Categories

The design of a terminal shall consider the environment in which the terminal is intended to operate. The terminal may either be designed to operate in a ‘normal’ attended shop–environment, or to operate in an unattended self–service environment.

A Flex–terminal must be designed to operate according to one (or more) of the following categories:

- Attended – with PIN Entry Device
- Unattended – with PIN Entry Device
- Unattended – without PIN Entry Device

The Terminal shall be able to present parameters showing the Terminal configuration. The parameters may e.g. be presented as a Terminal Report.

  

## 7.4 Choice of Business Call

Each time a new transaction (or a sequence of transactions) is initiated, a Business Call is required.

Six different Business Calls have been defined, and the use of these calls depends on the actual business situation.

If the final transaction amount is known when the transaction is initiated, the Business Call

- "Purchase"
- "Refund" (in case of credit transactions)

Concerning surcharges, please refer to section 7.24 (Addition of Surcharges and Fees).

If only an estimated amount is available when the transaction sequence is initiated, the Token based Business Calls shall be used:

- "Original Authorization",
- "Supplementary Authorization",
- "Capture" and
- "Reversal (Authorization)"

Depending on the business environment, the amount to be authorized shall be agreed by the individual acquirers.

(Support of Supplementary Authorization depends on the individual card schemes. Currently not supported by any card schemes).

**References**

Business Calls, definition: Section 6.2 (Business Calls) on page 6–14.

Terms – Business Calls and Administrative Functions: Attachment K.33

## 7.5 Refund

When a Refund transaction is going to be performed and the card contains several applications, the merchant shall (in a dialogue with the cardholder) decide which application to use.

Refund transactions are not applicable for unattended terminals and attended terminals performing cash or quasi–cash transactions.

The CVM selected for Refund transactions is always Signature. Unlike normal Purchase transactions, it is the merchant who shall sign the receipt handed over to the cardholder.

  

Cashback is not applicable for Refund transactions

**References**

Refund: section 6.2.6 on page 6–19.

## 7.6 Support of Card Technologies

Three different Card Data Sources (or card technologies) have been defined:

- ICC,
- Magnetic Stripe (Track 2) and
- Key–Entered

Presently, Key–Entry of card data is not supported.

A terminal able to accept Debit/Credit cards shall accept both ICC and Magnetic Stripe (including fallback from ICC) as card data source.

**References**

Card Data Source, definition: Section 9.2.15 on page 9–5.

## 7.7 ICC Technology and Fallback to Magnetic Stripe

When an ICC is inserted into the ICC reader, the terminal shall try to communicate with the ICC. This communication may fail, and fallback from ICC to Magnetic Stripe may be the only way to continue and complete the transaction.

If the terminal is attended and the terminal has separate ICC and Magnetic stripe readers, the merchant shall be able to testify that the ICC has been inserted correctly, before fallback to magnetic stripe may continue.

To be able to testify correct card entry, the Merchant Interface shall include two keys/menu items (“Yes”/“No”) to activate when the question “Card inserted correctly?” appears.

If the magnetic stripe is used and the magnetic stripe indicates that the card contains an IC, the terminal will reject the attempt and request the cardholder to use the ICC reader instead.

**References**

Fallback, description: Section 5.14 (Fallback from Chip (ICC) to Magnetic Stripe (MSC) on page 5–33.

  

Card inserted correctly: Section 5.14.2 on page 5–33.

## 7.8 Service Packs

In order to add new variants of existing commands and responses, the term Service Pack has been introduced.

To be able to utilize the new variants as defined by the Service Pack, it is essential that both the terminal and the PSAM supports the Service Pack.

A function has been defined, to make it possible for the terminal to decide the highest level of Service Packs supported by both entities.

**References**

Service Packs: Section 6.1.3 (Restart) on page 6–6

Service Packs: Section 11 (Service Packs)

## 7.9 Application Selection

When an ICC card is inserted in the terminal, the terminal builds the Candidate List. The Candidate List is the list of applications supported by both the actual ICC card and the terminal. The Candidate List may contain:

- No matching applications (i.e. the list is empty)
- One matching application
- More than one matching application.

If more than one matching application is found, the cardholder shall decide which application to be used. This selection shall be performed as a dialog between the cardholder and the terminal. The Merchant Interface may display to the merchant that an application selection or application acceptance is in progress and the cardholder action is awaited. The information displayed may include the application candidate(s).

If a Refund transaction is initiated, it is either the merchant or cardholder who shall decide the application to be used (if more matching applications have been identified). This may be implemented as a dialogue box (showing the Candidate List) on the Merchant Interface.

**References**

Application Selection: Section 5.13 (Application Selection) on page 5–22.

  

## 7.10 Support of Cardholder Verification Methods

The CVM (Cardholder Verification Method) to be used is decided by the PSAM. Based on the PSAM configuration, the Terminal Capabilities and data from the actual card, the PSAM will decide the actual CVM. That means that at the time of transaction initialization, the terminal will not know whether

- PIN,
- Signature,
- No CVM
- (or a combination of PIN and signature)

is going to be selected.

Default transactions shall be initialized without requesting any specific CVM, thus leaving the choice to the PSAM and card.

If the terminal is “Attended”, the terminal (incl. Merchant Interface) shall be able to support all the possible CVMs defined:

- PIN (online PIN or offline PIN verification),
- Signature,
- Combined (offline PIN and Signature) and
- No CVM.

If the terminal is “unattended”, the use of Signature as CVM is not relevant. Whether PIN is relevant or not, depends on whether a PIN Entry Device is present or not.

Some card schemes accept that the cardholder does not remember the PIN, even though these cards are expected to generate PIN–based transactions.

Dependent of which goods and services an unattended terminal delivers, PIN and/or No CVM may be supported.

To be able to support such customers, the Merchant Interface shall include a key/menu item to be activated when Signature shall be used instead of the CVM otherwise decided by the PSAM. The function to request a specific CVM is called “Forced CVM”.

The Merchant Interface may also include a key/menu item to give PIN priority as CVM.

The data element Merchant Initiative (bits 1, 2 and 8) is used to convey the request for a specific CVM to be used.

Whether the request for a specific CVM will be accepted or not, depends (among others) on the PSAM parameters and the actual card.

**References**

Forced CVM: Attachment O (Merchant Initiative Bypass).

Merchant Initiative, definition: Section 9.2.54 on page 9–13.

  

## 7.11 Temporary Offline Procedure

Card processing performed by the PSAM may imply that an online request shall be performed. If the terminal is not able to communicate with the host systems temporarily, e.g. due to technical problems in the communication network, the transaction (normally) fails. (The ASW1–ASW2 = '1618' (No host data received), received from the PSAM indicates that no host response is received).

If the terminal is not able to communicate with the host systems, the merchant may be able to initiate a transaction using a Temporary Offline Procedure. This procedure will indicate to the PSAM that the transaction processing shall be performed offline, i.e. without initiating an online request. Whether the procedure will be completed successfully or not, depends on the configuration of both the PSAM and the actual card. The function to request a transaction to be performed offline is called "Forced Offline".

To be able to use the Temporary Offline Procedure the Merchant Interface shall include a key/menu item to be activated when offline processing is requested.

The Merchant Interface may also include a key/menu item to request online processing.

The data element Merchant Initiative (bits 5, 6 and 7) is used to convey the request for a specific online/offline processing. Request for the Temporary Offline Procedure is indicated by the value '60' in Merchant Initiative.

When the merchant initiates the Temporary Offline Procedure the guarantee limit may differ from the general rules. The individual acquiring agreements, signed by the merchant and the acquirers, define the consequences.

If the merchant obtains an Approval Code e.g. making a phone call to acquirer's helpdesk, this may more or less compensate for the reduces guarantee.

How to obtain an Approval Code in case of temporary offline is described in section 7.12.

**References**

Merchant Initiative, definition: Section 9.2.54 on page 9–13.

  

## 7.12 Voice Authorization Calls

If the 'Temporary Offline Procedure' has been requested by the merchant, the merchant should be requested to make a manual Voice Authorization Call.

A Voice Authorization Call may be performed by calling the card issuers helpdesk (or voice response equipment) for an Approval Code. (The Approval Code consists of max. 6 alphanumeric characters.)

The request for Voice Authorization Calls may be combined with or replaced by a manual look up in a (paper based) Stop List (specific requirements may depend on the agreements between the merchant and the acquirer(s)).

The response to the request for a Voice Authorization Call may either be:

- No Voice Authorization Call Performed,
- No Voice Authorization Call Performed, but the card number is found in the (paper based) Stop List.
- Authorization Call performed, but the authorization request has been declined,
- Authorization Call performed, and the authorization request has been approved.

If the manual authorization request has been approved, an Approval Code has been received over the phone.

The merchant shall be able to select the appropriate response to the request, and if approved, be able to key–enter the Approval Code received.

The terminal solution may give the merchant the opportunity to switch off the request for a manual procedure. Instead of asking the merchant, an automatic answer (No Voice Authorization Call Performed) may be given.

In order to obtain a Voice Authorization, the PAN must be known. During the transaction, the PSAM/Terminal will inform the merchant about the actual PAN (to be provided in the *Check Stop List* command). This ensures that the PAN used origin from the correct application, especially in case of multi–application cards.

If the Voice Authorization Call is performed before the transaction is initiated, the PAN embossed on the card will be used. But in case of multi–application cards it may be impossible to visually read the PAN of the selected application.

**References**

Voice Authorization: Section 6.10.4 (EMV Payment) on page 6–44 and section 6.12.4 (MSC Payment) on page 6–70.

  

## 7.13 Stop List

If the terminal supports offline transactions, a Stop List may be implemented.

Normally the Stop List will be stored on the merchant operated part of the terminal solution, normally in the cash register system.

Updates to the Stop List, as well as a complete Stop List, shall be obtained directly from PBS by calling the dedicated platform for Stop List information. Normally it will be the cash register system that maintains the Stop List.

During transaction processing the PSAM will request for a look up on the Stop List in the following situations:

- If the actual card is an EMV card (also during online transactions), or
- If the transaction is processed offline (both MSC and EMV cards), e.g. due to requesting the 'Temporary Offline Procedure'.

The response to the request for look up on the Stop List depends on whether:

- No Stop List is available,
- Stop List is available, but the actual card number is not found in the list, or
- Stop List is available, and the actual card number is found in the list

If the actual card number is found in the Stop List, the list may indicate whether the card shall be picked–up (if possible) or just returned to the cardholder.

**References**

*Check Stop List* command: Section 8.6.18 on page 8–71.

## 7.14 Optimizing the Transaction Time

### 7.14.1 Parallel Processing

In general, the overall transaction time may be reduced if more tasks are performed in parallel. As an example, printing may be started before the entire contents is known and ICC data may be read by the terminal/PSAM while the merchant is calculating the transaction amount.

**Accelerated PIN Entry**

An example of parallel processing is that the cardholder may be prompted for PIN entry at an earlier point of time in the chip–

  

based transaction when compared to a straight–forward implementation.

Two different variants of such “Accelerated PIN Entry” (APE/DAPE) have been implemented in newer PSAM versions in order to speed up most transactions:

- APE, where PIN entry is requested after reading card data)
- DAPE (Dankort APE), where PIN entry is requested immediately after final application selection.

Terminals shall be able to handle the command flow depicted in table 6.14, which is fully in line with the TAPA architecture.

**Release of the ICC**

The terminal may release the card before the actual approval or denial of the transaction. The rules given in section 6.11.3 (Release of the ICC) shall be followed.

In this way, the cardholder can take the card in parallel with receipt printing.

### 7.14.2 Data Transmission

**Clock Frequency**

For both the ICC and PSAM interfaces, it is recommended to use the maximum frequency of 5 MHz. as defined in ref. 8: “ISO/IEC 7816–3” and ref. 36: “EMV, version 4.1”.

In this way, ICCs using the external clock for clocking the CPU will operate faster compared to the widely used frequency of 3.57 MHz.

Furthermore, data transmission to and from ICCs takes place at a bitrate directly proportional to the external clock frequency.

**NOTE:** Although the PSAM generates its own clock frequency internally, the overall transaction time will still benefit from a faster transmission rate when clocked at 5 MHz.

**I/O Buffer Sizes for T=0 (ICC interface)**

Terminal I/O buffer(s) should have sufficient length to avoid switching into single byte transmission (by use of procedure byte ‘60’) when conveying large messages.

**I/O Buffer Sizes for T=1 (ICC and PSAM interfaces)**

Terminal I/O buffer(s) should have sufficient length to avoid chaining at the T=1 level. This is especially the case for the PSAM interface where several messages during a transaction have the maximum size (length of the INF field is 254 bytes).

  

Terminal I/O buffer sizes different from the default value of 32 bytes shall be indicated to the ICC/PSAM by use of an S(IFS request) message issued after ATR and possibly PPS.

**Transmission Factors F and D (ICC interface)**

The time spent on data transmission on the ICC interface may be reduced for cards supporting bit rate adjustment factors (called "D") other than 1. Ref. 36: "EMV 4.1" requires terminals to support the values 1, 2 and 4 and cards to support the value 1 and optionally 2 and/or 4.

The method for negotiating values for F and D is Cold/Warm Reset.

**Transmission Factors F and D (PSAM interface)**

The time spent on data transmission on the PSAM interface may be significantly reduced when supporting bit rate adjustment factors (called "D") other than 1.

All PSAMs used for production support the values 1, 2, 4 and 12.

Presently, only FI=1 is supported by the PSAM indicating Fi=372 and $f_{max}$=5 MHz

The method for negotiating values for F and D is PPS ("Protocol and Parameters Selection") as defined in ref. 8: "ISO/IEC 7816–3".

**References**

Optimizing the Transaction Time: Section 6.11 (Optimizing the Transaction Time) on page 6–54.

## 7.15 Signature Verification and Accept

When signature is selected as CVM, the merchant may be requested to compare the cardholder's signature (just written on the receipt) with the reference signature on the card.

The configuration of the PSAM defines whether the question shall be asked to the merchant or not.

The terminal supplier may decide to permanently request signature verification to be performed, irrespective of the PSAM configuration.

To be able to accept or reject the cardholder's signature, the Merchant Interface shall include a pair of keys (Yes/No) to activate when the question "Signature accepted?" appears.

  

The CVM selected for Refund transactions is always Signature. Unlike normal Purchase transactions, it is the merchant who shall sign the receipt handed over to the cardholder.

**References**

Signature Verification: Section 6.4.2 (Signature) on page 6–26.

## 7.16 Receipts

The requirements state that the cardholder shall be able to get a receipt when that cardholder has accepted the transaction.

If the transaction is PIN based the cardholder accepts the transaction by entering the PIN and accepting the amount (by activating the Accept–key).

Since the cardholder accepts the transaction before the transaction result is known, a receipt shall be issued irrespective of the transaction result.

When PIN is used as CVM, the transaction may be rejected due to wrong PIN, and the cardholder will be requested to re–enter the PIN. If it is a magstripe transaction, the flow may continue after the PIN has been re–entered.

If the PIN has been online validated, a receipt shall be printed for each PIN entry.

If the PIN was offline validated and re–entered (early in the transaction sequence) the terminal must print at least one receipt (covering all PIN entry attempts).

If the transaction is signature based, the cardholder accepts the transaction by signing the receipt.

When a transaction is signature based, two receipts shall be printed. One to be signed by the cardholder and kept by the merchant, and one to be handed over to the cardholder.

If the function Signature Validation is enabled, and the merchant rejects the signature written, a receipt indicating that the transaction is rejected/cancelled due to “Signature Rejected” shall be printed and handed over to the cardholder. The cardholder receipt can therefore only be printed after the question “Signature accepted?” has been acted upon.

If the transaction is completed with No CVM (neither PIN nor signature), the cardholder (normally) accepts the transaction by accepting the amount. The cardholder just activates the Accept key when the amount appears in the display.

The cardholder shall get a receipt for each acceptance of the amount.

  

The terminal may print receipts in case of errors, rejections, cancellation, etc., even though a receipt is not required.

**References**

Receipts: Attachment G (Receipts)

## 7.17 Get Amount 2

Depending on the actual ICC card, the PSAM may request the amount to be determined at a very early stage of the transaction flow, and even before the card number (PAN) is known.

If the terminal supports Service Pack No. 1 (i.e. the *Get Amount 2* command is issued by the PSAM), the PAN–prefix will not be available in the command, in this situation. The field PAN–prefix will in this situation contain 4 bytes, each with the value ’00’.

If the PAN–prefix is not available in the *Get Amount 2* command (during an EMV transaction), and the terminal must know the actual type of card before the exact transaction amount can be determined, the terminal may generate a response saying that ‘the amount is not yet known’. Based on this response the transaction sequence will continue, and a second *Get Amount 2* command will be issued later on during the transaction, after the PAN–prefix is known.

**References**

*Get Amount 2* command: Section 11.4.2 (Get Amount 2).

## 7.18 Get Amount 3

If the PAN is unknown when the ICC card request the amount and the terminal supports Service Pack No. 2 (i.e. the *Get Amount 3* command is issued by the PSAM), the PAN will not be available in the command, in this situation. The $LEN_{PAN}$ will in this situation be equal to ‘00’ and the data element “Amount Request” will indicate “Initial Amount” It is then up to the terminal/Cashregister System to return either an estimated amount or an accurate amount.

If estimated amount is returned, the PSAM will issue a subsequent *Get Amount 3* command requesting an accurate amount.

**References**

*Get Amount 3* command: Section 11.5.1 (Get Amount 3) on page 11–5.

  

## 7.19 Transaction Result

During the processing of a transaction, the terminal sends 4 commands to the PSAM.

The 4 commands are:

- *Initiate Payment* command,
- *Payment* command,
- *Validate Data* command and
- *Complete Payment* command

Even though the receipt data may be available after the *Validate Data* command has been processed, the final transaction result will not be known until the response from the *Complete Payment* command is received from the PSAM.

**NOTE:** Not only the ASW1–ASW2 value '0000' returned from the PSAM indicates approved/successful. Also ASW values in the range '10XX' indicate approved/successful as defined in table 8.106.

When a terminal is interfaced to a cash register system or a similar equipment, it is very important that the design of the communication between the individual devices (i.e. protocol, message formats etc.) consider that communication problems may occur. A mechanism shall be built–in to overcome such problems and to ensure (among others) that the final transaction result is distributed to all relevant entities.

**References**

Transaction result: Section 6.18.2 (General Rules) on page 6–143 and section 8.8 (ASW1–ASW2 Coding) on page 8–92.

## 7.20 Transaction Checks

The PSAM offers two different features for avoiding situations where a cardholder pays twice for the same goods.

**Duplicate Transaction Check (PSAM)**

The PSAM is able to validate when a new transaction is identical to the last transaction completed successfully by the PSAM.

The PSAM will see a new transaction as identical to a previous transaction, if all the following conditions are fulfilled:

- The PANs are identical
- The amounts and currencies are identical
- The same type of Business Call is used (Purchase, Refund or Capture)

  

- No other transaction (of type Purchase, refund or Capture) has completed successfully since the first transaction
- The time between the two transactions is less than a specified time–out value.

If the new transaction is identified as identical to the previous, the new transaction will be rejected by the PSAM (ASW1–ASW2 = '1300' (Match on previous transaction)).

The default time–out value in which the check is active is 10 minutes.

Depending on the actual terminal environment, the terminal may modify the time–out value or disable the check.

**Status of Previous Transactions (Terminal)**

In excess of the control performed by the PSAM, the PSAM also offers a feature where the terminal and/or cash register system can request the status of a previously performed transaction having financial impact.

**NOTE:** A limited number of transactions are buffered for this check (typical 8 transactions).

**References**

Attachment Q (Status of Previous Transactions).

## 7.21 Log and Totals

A transaction log shall be maintained within the terminal or an interfaced cash register. The transaction log may either be stored in the terminal or in a cash register system interfaced to the terminal.

The transaction log is not only relevant for audit purposes and technical trouble–shooting, but also for settlement purposes and generating total reports.

Generally transaction messages may be divided into two main groups:

- Messages with no financial impact and
- Messages with financial impact.

Messages with no financial impact include (among other messages) Authorization Request messages, which may cause changes in the cardholders available amount limits, but no change on the account.

Messages with financial impact include (among other messages) Reversals, which may cause that an already registered message with financial impact shall be cancelled.

  

While messages with financial impact are stored locally in the terminal's Data Store, they will not be able to cause any changes on the cardholder's, nor the merchant's account. When a message with financial impact is transferred from the terminal to the host systems, the response to the terminal will include information relevant for the total reports generated by the terminal. The response data includes the card name and card group for totals, and indication of the actual settlement period.

Total reports shall be based on the messages with financial impact transferred from the terminal to the host systems, but the report may also reflect messages not yet transferred.

**References**

Log: section 5.4.3 (Log) and Attachment N (Guidelines for Constructing Total Reports).

## 7.22 Merchant Application Log

The Data Store in a terminal is used to store messages temporarily until they can be transferred to the host systems. All messages stored in the Data Store are generated by the PSAM.

The PSAM offers a function for automatic generation of a back–up of the Data Store. This back–up is directed to the merchant's side of the terminal equipment, e.g. in the cash register system. The Data Store back–up (or Merchant Application Log) receives a copy of all messages sent to the normal Data Store.

If the Data Store becomes defective, the messages stored in the Merchant Application Log may be used as back–up messages, and these messages may be delivered instead of the messages lost in the terminal's Data Store.

The terminal defines by the data element Info Level (bit 1) whether the PSAM shall store messages in the 'normal' Data Store only, or in both the Data Store and the Merchant Application Log.

**References**

Logging: Section 6.1.3 (Restart) on page 6–6.

## 7.23 Cashback Amount

The merchant may (depending on the agreements with the card schemes) disburse a cash amount (cashback) as a supplement to the amount for goods or services.

  

If the cashback function is implemented, the amount for cash should be included in the transaction amount transferred to the PSAM. The amount for cash should be indicated in the data element Amount Other as a subset of the transaction amount.

A cashback shall be indicated using the same Currency Code as used for the total transaction amount.

Currently, cashback is not supported by the host. Therefore, the data element Amount Other shall not contain any amount and the Transaction Type = '09' is not valid.

Despite cashback is not supported currently, the terminal may be able to invoke this functionality.

**References**

Cashback, definition: Section 9.2.7 (Amount, Other) on page 9–3.

## 7.24 Addition of Surcharges and Fees

The merchant (or the cash register) may add surcharges or other fees to the amount summed up for the goods or services.

Surcharging or fees shall be added before the transaction amount is determined and transferred to the PSAM. When the cardholder accepts a transaction, e.g. by entering the PIN or signing a receipt, the total amount shown shall include surchanging and other fees.

**References**

Surcharges and Fees: Section 6.3 (Gratuity and other surcharges) on page 6–20.

## 7.25 Gratuity

In certain environments the Cardholder may add gratuity/tips to the amount summed up for the goods or services.

Like for surcharges and fees, the total amount displayed during PIN entry shall include any gratuity. It means that the gratuity amount shall be agreed before PIN entry.

If the transaction is signature based, the receipt may contain space for the Cardholder to add the gratuity.

**References**

Surcharges and Fees: Section 6.3 (Gratuity and other surcharges) on page 6–20.

  

## 7.26 Dual Communication Access Points

During the processing of a transaction, the PSAM may initiate an online request to be executed, before the transaction processing is able to complete. To be able to execute the online request, the terminal shall be able to establish a connection to the host systems.

If the merchant initiates any of the administrative functions, e.g. Advice Transfer Request, a connection to the host systems shall be established too.

Irrespective of the background for establishing a connection to the host systems, the request for connection shall be performed identical.

To be able to offer the highest level of availability, PBS has established two identical platforms. Each platform has its own communication lines to the external communication networks. Both platforms are active 24 hours per day.

Each platform has its own address. If a switched communication network is used (e.g. PSTN or ISDN), the two platforms shall be called using different call numbers. The two platforms are also identified by individual IP–addresses.

To be able to utilize the increased availability, obtained by the dual host platforms, the terminals shall be able to initiate a connection to the second platform, if a request for connect fails while trying to connect to the first platform.

The algorithm used to select which platform to call first, shall consider an equal load on both platforms in normal situations, and the algorithm shall also provide the necessary functionality to handle situations when one of the platform is inaccessible.

**References**

Terminal Operator Communication Access Points: section 6.17.5 and Dual access points: Section F.3 (Communication Protocols).

## 7.27 Automatic Advice Transfer if no Customers being Serviced

For attended terminals an Advice Transfer is normally initiated by the merchant or as a result of an action performed by the merchant, e.g. log–in/Log–out to the cash register.

An Advice Transfer shall be initiated frequently, and at least once a day. An Advice Transfer initiated by the merchant is fol-

  

lowed by a PSAM Update sequence to ensure that the PSAM contains the latest configuration parameters.

Since no merchant is present at unattended terminals, the Advice Transfer and PSAM Update sequences shall be initiated automatically.

The Advice Transfer is also defined as the function to initiate balancing. Beyond that the Advice Transfer also contributes to minimize the risk for losing any advices while stored in the Data Store.

Further improvements for minimizing the risk for losing advices may be implemented, e.g. if the terminal automatically initiates an Advice Forwarding, a predefined number of minutes after the last transaction has been performed.

In this situation the Advice Forwarding shall not be initiated if the Data Store is empty, likewise the PSAM Update sequence shall be omitted.

The purpose of this automatic initiated Advice Forwarding is exclusively to empty the Data Store, not to initiate any balancing or PSAM update sequences.

**References**

Advice Transfer: Section 6.16.4 (Advice Transfer), 6.16.5 (Advice Enclosing) and 6.16.6 (Advice Forwarding).

## 7.28 Host Messages

Each response from the host may contain additional information addressed to the merchant.

The Host has the possibility to add a text message to the Merchant Display (Tag ’CA’), or a request for an Advice Transfer (Tag ’C9’).

How the terminal reacts to Tag ’C9’ may depend on the actual implementation. An unattended terminal may be able to act automatically when e.g. a request for Advice Transfer is received.

**References**

Section F.7 (Primitive Data Objects for the APACS Header) on page F–14.

  

## 7.29 Transaction State Information

The PSAM offers a service to keep the merchant informed of the current state during the transaction.

The terminal defines by the data element Info Level (bit 2) whether the PSAM shall send Message Codes to the Merchant Application Handler (Merchant Interface).

**References**

PSAM State Information: Section 6.1.3 (Restart) on page 6–6.

Transaction State Information, command: Section 8.6.21 on page 8–76.

## 7.30 Local PIN

The PSAM offers a functionality where a reference PIN is conveyed to the PSAM (in plaintext or enciphered) and compared internally with a PIN entered on the PIN Entry Device (PED) by the cardholder. The PSAM will return the result of the comparison.

Both plaintext or enciphered reference PIN can be used. It is recommended to use the enciphered reference PIN, as this solution enhance the security by offering confidentiality and reduce the possibility for performing replays. This is accomplished by adding a validation of a transaction counter given by the Local PIN application with the transaction counter maintained by the PSAM.

**References**

Attachment P (Local PIN).

Commands: Section 8.7 (Local PIN Commands) on page 8–86.

Data Elements: Section 9.3 (Data Elements specific for the Local PIN Application) on page 9–25.

ASW1–ASW2: Section 8.8.2 (ASW1–ASW2 Applicable for Local PIN) on page 8–138**.**

## 7.31 Certification

The basic certification of EMV functionality (level 1 & 2) shall be performed by an EMV accredited test house e.g. Delta in Denmark.

  

Before an EMV level 2 certification is initiated, the terminal vendor shall determine the number of business and technical functions supported e.g. PIN code, signature, attended/unattended (stated in an Implementation Conformance Statement (ICS)).

Each terminal or terminal solution shall subsequently be certified according to the requirements defined by the card schemes and the requirements stated in the OTRS.

A terminal may be certified as a stand alone terminal. A terminal can also be a part a terminal solution interfacing a cash register system.

If a terminal solution is based on a previously certified terminal, a supplementary certification of the complete solution is required. The volume of the supplementary certification depends on the level of new and not yet certified hardware and software components.

When an EMV level 2 certified terminal is part of terminal solution, the terminal solution shall support the same number of business and technical functions as defined for the terminal.

## 7.32 Cash/Quasi–Cash Terminals

The following combinations of Terminal Types and Transaction Types are supported:

Table 7.1 – Cash/Quasi–Cash Terminals

| Terminal Type | Transaction Type | Trade |
|---|---|---|
| 11 (Cash, Financial Institution) | 01 (Cash) | Banks & savings banks (6010) |
| 21 (Quasi–Cash) | 11 (Quasi–Cash) | Gambling & Casino (7995)<br>Exchange bureau (6051)<br>Post office (4829) |

Cash/Quasi–Cash Terminals have the following limitations:

- Cash transactions are *always* performed online
- PIN and Signature are allowed as CVM
- Refund transactions is *not* allowed
- Cash/Quasi–Cash can *not* be combined with Goods and Services

Table 7.2 – Cash/Quasi–Cash – Applicable Business Calls

| Terminal Type | Purchase | Original Authorization | Capture |
|---|---|---|---|
| 11 (Cash, Financial Institution) | ● | ● | ● |
| 21 (Quasi–Cash) | ● | | |

  

## 7.33 POS Terminal/CAT Levels vs. Terminal Type

The following four tables (7.3 – 7.7) can be used to find the outer boundaries for a specific Terminal Type regarding offline/online transactions, CVM, Transaction Requests and Transaction Type.

Note that terminals may be limited further due to specific restrictions (international as well as national). Therefore, it is highly recommended to contact PBS before finalizing the terminal functionality design.

**NOTE:** Signature only terminals are *not* allowed according to MasterCard International and Visa International rules.

Table 7.3 – Online/Offline Transactions Vs. Terminal Type

| **Transaction** | | **MSC** | | **ICC** | | **Key–entered** | |
|---|---|---|---|---|---|---|---|
| **Terminal Type** | | Online | Offline | Online | Offline | Online | Offline |
| Attended – Financial Institution controlled | | | | | | | |
| 11 | Online | ● | | ● | | | |
| 12 | Online capable | | | | | | |
| 13 | Offline | | | | | | |
| Unattended – Financial Institution controlled | | | | | | | |
| 14 | Online | | | | | | |
| 15 | Online capable | | | | | | |
| 16 | Offline | | | | | | |
| Attended – Merchant controlled | | | | | | | |
| 21 | Online | ● | | ● | | | |
| 22 | Online capable | ● | ● | ● | ● | | |
| 23 | Offline | | | | | | |
| Unattended – Merchant controlled | | | | | | | |
| 24 | Online | ● | | ● | | | |
| 25 | Online capable | ● | ● | ● | ● | | |
| 26 | Offline | | ● | | ● | | |
| Unattended – Cardholder controlled | | | | | | | |
| 34 | Online | | | | | | |
| 35 | Online capable | | | | | | |
| 36 | Offline | | | | | | |

**Legend:** ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.

  

Table 7.4 – CVM Vs. Terminal Type

| CVM | | PIN | | Signature[1)] | | No CVM | |
|---|---|---|---|---|---|---|---|
| **Terminal Type** | | Online[2)] | Offline[2)] | Online | Offline | Online | Offline |
| Attended – Financial Institution controlled | | | | | | | |
| 11 | Online | ● | | ●[3)] | | | |
| 12 | Online capable | | | | | | |
| 13 | Offline | | | | | | |
| Unattended – Financial Institution controlled | | | | | | | |
| 14 | Online | | | | | | |
| 15 | Online capable | | | | | | |
| 16 | Offline | | | | | | |
| Attended – Merchant controlled | | | | | | | |
| 21 | Online | ● | | ● | | | |
| 22 | Online capable | ● | ● | ● | ● | ● | ● |
| 23 | Offline | | | | | | |
| Unattended – Merchant controlled | | | | | | | |
| 24 | Online | ● | | | | | |
| 25 | Online capable | ● | ● | | | ● | ● |
| 26 | Offline | | | | | | ● |
| Unattended – Cardholder controlled | | | | | | | |
| 34 | Online | | | | | | |
| 35 | Online capable | | | | | | |
| 36 | Offline | | | | | | |

**Legend:** ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.

1) = Signature only terminals are not allowed.

2) = Indicates whether the transaction has been performed online or offline. Does *not* implicate whether online PIN verification or offline PIN verification is performed.

3) = In case of Cash terminals, the use of signature as CVM can be disabled by PBS.

Table 7.5 – Transaction Request Vs. Terminal Type

| **Transaction Request** | | **Purchase** | **Refund[1)]** | **Org. Auth.** | **Supp. Auth.** | **Capture** | **Rev. (Auth.)** |
|---|---|---|---|---|---|---|---|
| **Terminal Type** | | '00' | '01' | '02' | '03' | '04' | '05' |
| Attended – Financial Institution controlled | | | | | | | |
| 11 | Online | ● | | ● | | ● | ● |
| 12 | Online capable | | | | | | |
| 13 | Offline | | | | | | |
| Unattended – Financial Institution controlled | | | | | | | |
| 14 | Online | | | | | | |
| 15 | Online capable | | | | | | |
| 16 | Offline | | | | | | |
| Attended – Merchant controlled | | | | | | | |
| 21 | Online | ● | | | | | |
| 22 | Online capable | ● | ● | ● | | ● | ● |
| 23 | Offline | | | | | | |
| Unattended – Merchant controlled | | | | | | | |
| 24 | Online | ● | | ● | | ● | ● |
| 25 | Online capable | ● | | ● | | ● | ● |
| 26 | Offline | ● | | | | | |
| Unattended – Cardholder controlled | | | | | | | |
| 34 | Online | | | | | | |
| 35 | Online capable | | | | | | |
| 36 | Offline | | | | | | |

**Legend:** ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.

[1)] = For Cash terminals, Refund transactions are not allowed.

Table 7.6 – Transaction Type Vs. Terminal Type

| Transaction Type | | Goods & Services | Cash[1)] | Goods & Services with Cash-disburse-ment | Quasi–Cash and scrip | Returns/ Refunds |
|---|---|---|---|---|---|---|
| **Terminal Type** | | '00' | '01' | '09' | '11' | '20' |
| Attended – Financial Institution controlled | | | | | | |
| 11 | Online | | ● | | | |
| 12 | Online capable | | | | | |
| 13 | Offline | | | | | |
| Unattended – Financial Institution controlled | | | | | | |
| 14 | Online | | | | | |
| 15 | Online capable | | | | | |
| 16 | Offline | | | | | |
| Attended – Merchant controlled | | | | | | |
| 21 | Online | | | | ● | |
| 22 | Online capable | ● | | | | |
| 23 | Offline | | | | | |
| Unattended – Merchant controlled | | | | | | |
| 24 | Online | ● | | | | |
| 25 | Online capable | ● | | | | |
| 26 | Offline | ● | | | | |
| Unattended – Cardholder controlled | | | | | | |
| 34 | Online | | | | | |
| 35 | Online capable | | | | | |
| 36 | Offline | | | | | |

**Legend:** ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.

[1)] = For Cash terminals, Refund transactions are not allowed.

Table 7.7 – Terminal Types

| Terminal Type | | Transaction Request | | Transaction Type | | Terminal Capabilities |
|---|---|---|---|---|---|---|
| **Attended – Financial Institution Controlled** | | | | | | |
| TERM11 | Online only | TR00 | Purchase | TT01 | Cash | All CVMs except No CVM |
| | | TR02 | Original Authorisazion | TT01 | Cash | All CVMs except No CVM |
| | | TR04 | Capture | TT01 | Cash | All CVMs except No CVM |
| **Attended – Merchant Controlled** | | | | | | |
| TERM21 | Online only | TR00 | Purchase | TT11 | Quasi–Cash | All CVMs except No CVM |
| TERM22 | Offline with online Capability | TR00 | Purchase | TT00 | Goods and Services | All CVMs |
| | | TR01 | Refund | TT20 | Refunds | Signature only (Merchant) |
| | | TR02 | Original Authorization | TT00 | Goods and Services | All CVMs |
| | | TR04 | Capture | TT00 | Goods and Services | All CVMs |
| | | TR05 | Reversal | TT00 | Goods and Services | – |
| **Unattended – Merchant Controlled** | | | | | | |
| TERM24 | Online only | TR00 | Purchase | TT00 | Goods and Services | Online PIN only |
| | | TR02 | Original Authorisazion | TT00 | Goods and Services | Online PIN only |
| | | TR04 | Capture | TT00 | Goods and Services | Online PIN only |
| | | TR05 | Reversal | TT00 | Goods and Services | – |
| TERM25 | Offline with online Capability | TR00 | Purchase | TT00 | Goods and Services | Online PIN & offline PIN |
| | | TR02 | Original Authorisazion | TT00 | Goods and Services | Online PIN & offline PIN |
| | | TR04 | Capture | TT00 | Goods and Services | Online PIN & offline PIN |
| | | TR05 | Reversal | TT00 | Goods and Services | – |
| TERM25 | Offline with online Capability | TR00 | Purchase | TT00 | Goods and Services | No CVM |
| TERM26 | Offline only | TR00 | Purchase | TT00 | Goods and Services | No CVM |

This page is intentionally left blank

  